We Claim:

1. A method of detecting a rogue access point comprising the steps of:

directing a packet from a supplicant to a network through an access point;

receiving a network response packet by the supplicant from the access point;

determining whether the access point is one of a valid network access point is one of a valid network access point and a rogue access point based on whether the network response packet received from the access point is respectively in one of conformity and nonconformity with predetermined expectations.

2. The method of claim 1 wherein, if the access point is determined to be a valid network access point, further comprising the step of authenticating the supplicant to the network.

3. The method of claim 1 wherein, if the access point is determined to be a rogue access point, further comprising the step of reporting the rogue access point to the network.

4. The method of claim 3 wherein the step of reporting comprises contacting the network by the client through a valid network access point.

5. The method of claim 1 wherein the predetermined expectations comprise data traffic conforming with IEEE 802.1X standards.

6. The method of claim 1 wherein the predetermined expectations comprise a mutual authentication to the network, wherein non-conformity is determined by a failure of the mutual authentication.

7. The method of claim 6 wherein the mutual authentication comprises:

issuing a challenge from the server to the client;

issuing a counter-challenge from the client to the server;

wherein mutual authentication fails at the counter-challenge since the access point's username and password are not found in the server's database.

8. The method of claim 6 wherein the mutual authentication comprises:

directing a message containing identity credentials from the supplicant, through the access point, to an authentication server;

validating the identity credentials of the supplicant using the authentication server;

forwarding a send key from the authentication server to the supplicant through the access point;

independently deriving a session key from the send key and the identity credentials by the supplicant and the authentication server;

encrypting data packets between the supplicant and the authentication server using the derived session key.

9. The method of claim 8 wherein the credentials are a username/password combination.

10. The method of claim 8 further comprising:

prior to the step of directing, sending a start message from the supplicant to the access point;

sending an identity request message from the access point to the supplicant; and

wherein the step of directing a message comprises sending an identity response message containing the identity credentials form the supplicant to the access point in response to the identity request message, and forwarding the identity response message from the access point to the authentication server.

11. The method of claim 10 wherein the authentication server is a RADIUS server and wherein the identity response message is in the form of a RADIUS access request, wherein the method further comprises the steps of:

responding to the RADIUS access request with a RADIUS challenge from the authentication server to the supplicant; and responding from the supplicant to the RADIUS challenge according to the RADIUS protocol.

12. The method of claim 11 wherein the steps of validating and forwarding comprise sending the supplicant a RADIUS accept message and wherein the send key comprises an MS-MPPE-Send-key.

13. The method of claim 8 wherein the step of forwarding a send key comprises supplying key length and key index to specify encryption parameters for the session key.

14. The method of claim 10 wherein the encryption parameters are based on one of a 40/64-bit and a 104/128-bit key.

15. The method of claim 8 further comprising the initial step of configuring the supplicant in a device mode where the identity credentials are stored on a network card for non-interactive authentication by a user.

16. The method of claim 8 further comprising the initial step of configuring the supplicant in a network logon mode where the identity credentials are integrated into a network logon to enable a single sign-on for network authentication and PC network logon.

17. The method of claim 8 further comprising the initial step of establishing authenticator support comprising:

configuring the access point to use one of 40/64-bit and 104/128-bit WEP mode; and

providing the access point with the authentication server address and encryption scheme to be used for communication.

18. The method of claim 8 further comprising the initial step of establishing the authentication server comprising:

setting up a user database selected from at least one of a local database and a network database; and

setting up the access point as a network access server.

19. The method of claim 8 wherein the supplicant, access point and authentication server are part of a wireless local area network.

20. The method of claim 8 wherein the supplicant, access point and authentication server are part of a hard-wired local area network.

21. An arrangement for detecting a rogue access point comprising:

means for directing a packet from a supplicant to a network through an access point;

means for receiving a network response packet by the supplicant from the access point;

means for determining whether the access point is one of a valid network access point is one of a valid network access point and a rogue access point based on whether the network response packet received from the access point is respectively in one of conformity and nonconformity with predetermined expectations.

22. The arrangement of claim 21 further comprising means for authenticating the supplicant to the network, if the access point is determined to be a valid network access point.

23. The arrangement of claim 21 further comprising means for reporting the rogue access point to the network, if the access point is determined to be a rogue access point.

24. The arrangement of claim 3 wherein the means for reporting comprises means for contacting the network by the client through a valid network access point.

25. The arrangement of claim 21 wherein the predetermined expectations comprise data traffic conforming with IEEE 802.1X standards.

26. The arrangement of claim 1 wherein the predetermined expectations comprise a mutual authentication to the network, wherein non-conformity is determined by a failure of the mutual authentication.

27. The arrangement of claim 21 wherein the means for mutual authentication comprises:

means for directing a message containing identity credentials from the supplicant, through the access point, to an authentication server;

means for validating the identity credentials of the supplicant using the authentication server;

means for forwarding a send key from the authentication server to the supplicant through the access point;

means for independently deriving a session key from the send key and the identity credentials by the supplicant and the authentication server;

means for encrypting data packets between the supplicant and the authentication server using the derived session key.

28. The arrangement of claim 27 wherein the credentials are a username/password combination.

29. The arrangement of claim 27 further comprising:

prior to the means for directing, providing means for sending a start message from the supplicant to the access point;

means for sending an identity request message from the access point to the supplicant; and

wherein the means for directing a message comprises means for sending an identity response message containing the identity credentials form the supplicant to the access point in response to the identity request message, and means for forwarding the identity response message from the access point to the authentication server.

30. The arrangement of claim 29 wherein the authentication server is a RADIUS server and wherein the identity response message is in the form of a RADIUS access request, wherein the arrangement further comprises:

means for responding to the RADIUS access request with a RADIUS challenge from the authentication server to the supplicant; and means for responding from the supplicant to the RADIUS challenge according to the RADIUS protocol.

31. The arrangement of claim 29 wherein the means for validating and forwarding comprise means for sending the supplicant a RADIUS accept message and wherein the send key comprises an MS-MPPE-Send-key.

32. The arrangement of claim 27 wherein the means for forwarding a send key comprises means for supplying key length and key index to specify encryption parameters for the session key.

33. The arrangement of claim 32 wherein the encryption parameters are based on one of a 40/64-bit and a 104/128-bit key.

34. The arrangement of claim 27 wherein the supplicant, access point and authentication server are part of a wireless local area network.

35. The arrangement of claim 27 wherein the supplicant, access point and authentication server are part of a hard-wired local area network.